This application is submitted in the name of inventors Aravind Sitaraman and Shujin Zhang, assignors to Cisco Technology, Inc., a California Corporation.

SPECIFICATION

TITLE OF INVENTION

IP ADDRESS ALLOCATION IN A NETWORK ENVIRONMENT

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to providing a user with an Internet protocol (IP) address in a network environment. More particularly, the present invention relates to providing an IP address from an Internet service provider to a user via a network access provider in a dynamic and scalable manner.

Background

Dial-up, ISDN (integrated services digital network) and DSL (digital subscriber line) services provide for Internet access by transmitting data over existing twisted pair telephone lines to a central office of the telecommunications loop provider where the subscribers physically connect to a network access provider (NAP) and send and receive data communications to the Internet via a network access server (NAS) using, for example, point-to-point protocol. In order to use the Internet, the user typically must obtain an IP address from a local pool at the Point of Presence (POP) maintained by the NAP that the user connects to, or the user must obtain an IP address from a home

gateway server (HGS) at an Internet service provider (ISP). Often, the ISP and the NAP are separate entities, both physically and organizationally.

When the ISP and NAP are separate, there is a need to provide the subscriber, or user, with an IP address from the HGS via the NAS. Two methods are currently used.

One existing method involves manual planning of the IP address allocation between the NAP and the ISP. In this method, the ISP gives a block of IP addresses to the NAP, and the NAP configures the NAS with the block of IP addresses so that the NAS may give them out. The addresses are available to the user directly from the NAS. However, both the NAP and the ISP must agree to share the same routing protocols, which may be undesirable. The approach is also administratively complex and time consuming because any change in IP address allocation will result in a need to reconfigure all the network access servers involved and many network access servers may need to be reconfigured.

A second existing method involves tunneling IP address requests from the NAS to the home gateway server (HGS) of the ISP. This avoids route-sharing and administrative complexity. However, the tunneling method is not truly scalable because the HGS must maintain information for each individual tunnel that may be established. Currently, there is no HGS that can scale up to expected demand.

Because of the limitations of the existing methods, there is a need for providing an IP address from an ISP to a user via a NAS in a dynamic and scalable manner.

BRIEF DESCRIPTION OF THE INVENTION

A network access server (NAS) provides a connection to a user in a data communications network, where the NAS is capable of communicating with a home gateway server (HGS) maintaining a pool of IP addresses for allocation to authorized users associated with the NAS. The NAS includes a first memory for storing an identification of a user, a requester for asking the HGS for an IP address on behalf of the user; and a second memory associated with the first memory for storing the IP address of the user received from the HGS. The NAS may further include a detector for periodically detecting connection of the user to the NAS and a keep-alive sender for periodically informing the HGS that the user is still connected to the NAS, a receiver for receiving periodic queries from the HGS about the status of the user connection to the NAS and a responder responsive to said periodic queries for informing the HGS that the use is still connected to the NAS, and/or a receiver for receiving periodic signals from the user and a forwarder responsive to said receiver for forwarding information to the HGS that the user is still connected to the NAS. A home gateway server (HGS) provides mechanisms to assign an IP address to a user via a NAS, and to monitor the status of the IP address after assignment.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram showing the functional components of a network access server in accordance with a specific embodiment of the present invention.

FIG. 2 is a block diagram showing the functional components of a home gateway server in accordance with a specific embodiment of the present invention.

FIG. 3 is a process flow diagram showing the processes between and within a user, a network access server, and a home gateway server in accordance with a specific embodiment of the present invention.

FIG. 4 is a process flow diagram showing the processes between and within a user, a network access server, and a home gateway server if the connection between the NAS and the user is intentionally terminated by the user in accordance with a specific embodiment of the present invention.

FIG. 5 is a process flow diagram showing the processes between and within a user, a network access server, and a home gateway server when NAS keep-alive sender is used to monitor the status of an IP address in accordance with a specific embodiment of the present invention.

FIG. 6 is a process flow diagram showing the processes between and within a user, a network access server, and a home gateway server when a HGS query sender is used to monitor the status of an IP address in accordance with a specific embodiment of the present invention.

FIG. 7 is a process flow diagram showing the processes between and within a user, a network access server, and a home gateway server when a user-originated in-use message is used to monitor the status of an IP address in accordance with a specific embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Those of ordinary skill in the art will realize that the following description of the present invention is illustrative only and not in any way limiting. Other embodiments of the invention will readily suggest themselves to such skilled persons having the benefit of this disclosure.

FIG. 1 is a block diagram showing the functional components of a network access server (NAS) in accordance with a specific embodiment of the present invention. The NAS (10) is capable of communicating with a user via a first port (12). The NAS is capable of communicating with a remote server such as a HGS via a second port (14). The NAS has a memory (16), including a memory for storing a user identification (18) and a memory for storing an IP address associated with the user (20).

Typically, the user has a contractual relationship with an Internet service provider (ISP) which provides the user with an IP address through an HGS. The user will initiate a connection with the NAS over a telephone line, ISDN line or DSL line. The user may transmit authenticating information such as a user identification and password to a requester (24). The authenticating information may be stored in memory (16).

The NAS (10) has a HGS identifier (22) which uses available information about the user to determine the identity of the HGS associated with the user. Available information may include the authenticating information such as the user name and fully qualified domain name (FQDN), e.g., Joe@isp.net, or may include the phone number of

the user, using caller ID, for example. In any event, the HGS identifier (22) determines the identity of the destination HGS in some fashion and communicates with the requester (24). The destination HGS may be stored in memory (16).

The requester (24) obtains the authenticating information and the identity of the HGS, and contacts the HGS and requests an IP address on behalf of the user. If the user is authenticated, the HGS will, among other things, transmit an IP address which is received by the relayer (26) at the NAS (10). The relayer (26) causes the IP address to be stored in memory (20) and relays the IP address to the user.

The user's connection with the Internet must go through the NAS (10). The NAS (10), therefore, is positioned to monitor the status of the user's Internet connection. The NAS (10) is also positioned to provide this status information to the HGS.

If the user wishes to intentionally stop the Internet connection, the user sends a disconnection request which is received by a generator (28). Then, the generator (28) responds to the receipt of the disconnection request from the user by generating and sending a notice to the HGS that the user is no longer connected to the NAS (10). The generator (28) also causes memory (16) to be updated, including updating of routing tables where appropriate.

The NAS (10) may also include mechanisms to inform the HGS of unintentional disconnection of the user. The NAS (10) has a detector (30) which monitors the

connection between the user and the NAS (10). While the connection continues, the detector (30) may cause a keep-alive sender (32) to send periodic keep-alive messages to the HGS. These keep-alive messages indicate to the HGS that the user is using the IP address. If the connection is lost, the absence of periodic keep-alive messages will cause the HGS to de-allocate the IP address from the disconnected user and put it back in the pool for reallocation. If the connection is lost, the detector will also cause memory (16) to be updated.

Alternatively, instead of the NAS (10) sending keep-alive messages, the HGS may periodically query the NAS (10) or the user to verify that the user (and the NAS) is still connected. If the HGS queries the NAS (10), a query receiver (34) will receive the query and communicate with the detector (30). Then, if the connection is existing, the query receiver (34) will cause a responder (36) to send a message to the HGS indicating that the IP address is still in use. If the HGS queries the user, the query receiver (34) will receive the query and forward it to the user. Then, if the connection is existing, the user will send an in-use message to the in-use receiver (38) at the NAS (10) and the message will be forwarded to the HGS by a forwarder (40). If, for any reason, the query of the HGS is not affirmed, the HGS will de-allocate the IP address from the user and put it back in the pool for reallocation.

In another alternative, the user may be responsible for initiating periodic in-use messages to inform the HGS of an ongoing connection. In this instance, an in-use receiver (38) at the NAS (10) will receive the periodic messages and they will be

forwarded to the HGS by the forwarder (40). If, for any reason, the periodic in-use messages are not received by the HGS, the HGS will de-allocate the IP address from the user and put it back in the pool for reallocation.

FIG. 2 is a block diagram showing the functional components of a home gateway server (HGS) in accordance with a specific embodiment of the present invention. The HGS (50) has a port (52) for communicating with a NAS. The HGS also has an IP address pool maintainer (56) for maintaining a pool of IP addresses for allocation to users and a user identification maintainer (58) for maintaining the status of an active user. The IP address pool maintainer (56) maintains access to a pool of IP addresses. Such pool of IP addresses may be stored in memory within the HGS or, alternatively, the IP address pool maintainer may provide functionality to allow access to a pool of IP addresses stored in memory at a remote server such as a RADIUS server. The user identification maintainer (58) stores identification information (such as a user name and password) associated with an active user. The user identification maintainer (58) provides functionality to allow an active user to continue to use his or her allocated IP address. The HGS also includes a memory (60) for storing an IP address allocated to the user.

A primary function of the HGS (50) is to allocate IP addresses to authorized users. The HGS (50) has access to a pool of IP addresses via an IP address pool maintainer (56). The HGS can access information pertaining to authorized users who are eligible to be allocated IP addresses through an authenticator (62). When an IP address is requested for a user, the authenticator (62) determines if the user is eligible for an IP

address. If the user is eligible, an IP is allocated from the pool. Allocation includes updating the user identification maintainer (58) to indicate that a particular user is using the address and updating the IP address pool maintainer (56) to indicate that the address is not currently available for use by other users.

Updating memory may also include updating routing tables, where appropriate, since the HGS may perform routing functions using the IP addresses.

In allocating an IP address, the HGS (50) establishes communication with a NAS via the port (52). An authenticator (62) receives a request for an IP address for a user, an identification of the user, and authenticating information associated with the user. The identification and authenticating information as received may be stored in memory. The authenticator (62) provides functionality to compare the authenticating information with an authorized user database. Parts of the authenticating process, such as comparing the authenticating information to an authorized user database, may be proxied to another server. Also, for example, the authorized user database may be stored in a remote server.

If the authenticating information is correct, the authenticator (62) causes the allocator (64) to allocate an IP address to the user from the pool of IP addresses maintained by the IP address pool maintainer (56). As described above, the HGS may obtain the IP address either locally or from a remote server. The IP address is stored in memory (60) and other data associated with the user is stored in the user identification

maintainer (58). Once the IP address has been allocated, an IP address sender (66) sends the IP address to the NAS, which in turn will send the IP address to the user.

Once the IP address has been allocated to the user, the HGS (50) must monitor whether use of the IP address is continuing. In one embodiment, a keep-alive receiver (70) receives periodic keep-alive messages from the NAS indicating that the user is continuing to use the IP address. The keep-alive receiver (70) communicates with the user identification maintainer (58) to ensure that the IP address remains allocated to the user for as long as the keep-alive messages continue. As discussed above, the keep-alive messages are initiated by the NAS.

In another embodiment, an in-use receiver (76) receives keep-alive messages from the user via the NAS indicating that the user is continuing to use the IP address. The in-use receiver (76) communicates with the user identification maintainer (58) to ensure that the IP address remains allocated to the user for as long as the in-use messages continue. As discussed above, the in-use messages are initiated by the user.

In yet another embodiment, the HGS (50) has a query sender (72) which periodically queries either the NAS or the user whether the IP address is still in use. As discussed above, when the NAS is queried the NAS responder may send a message to the HGS (50) indicating that the IP address is still in use. Also as discussed above, when the user is queried the NAS generator may send a message to the HGS (50) indicating that the IP address is still in use. If the messages are in response to a query by the HGS (50),

the messages are received by a response-to-query receiver (74). The response-to-query receiver (74) communicates with the user identification maintainer (58) to ensure that the IP address remains allocated to the user for as long as the response-to-query messages continue.

De-allocation of an IP address involves returning the IP address to the IP address pool and updating the user identification maintainer (58) to indicate that the IP address is no longer being used by the user. Updating memory may also include updating routing tables.

The HGS (50) has mechanisms for de-allocating the IP address from the user and returning the IP address to the pool of IP addresses (56). In one mechanism, a disconnect notice receiver (68) receives a disconnect notice from the NAS. Then, the disconnect notice receiver (68) causes de-allocation of the IP address from the user by updating memory (60) and the user identification maintainer (58) to indicate that the user is no longer active and by causing return of the IP address to the pool of IP addresses maintained by the IP address maintainer (56).

In another mechanism, the keep-alive receiver (70) stops receiving keep-alive messages. Since the keep-alive messages are expected by the keep-alive receiver (70) periodically, the keep-alive receiver (70) is aware when a message is expected but not received. For example, if a message related to a user's IP address is expected every second, and a message has not been received for five seconds, the keep-alive receiver

(70) can recognize this and respond accordingly. When the keep-alive receiver (70) stops receiving the keep-alive messages, it causes de-allocation of the IP address from the user by updating memory (60) and the user identification maintainer (58) to indicate that the user is no longer active and by causing return of the IP address to the pool of IP addresses maintained by the IP address maintainer (56).

In another mechanism, the in-use receiver (76) stops receiving in-use messages. Since the in-use messages are expected by the in-use receiver (76) periodically, the in-use receiver (76) is aware when a message is expected but not received. When the in-use receiver (76) stops receiving the in-use messages, it causes de-allocation of the IP address from the user by updating memory (60) and the user identification maintainer (58) to indicate that the user is no longer active and by causing return of the IP address to the pool of IP addresses maintained by the IP address maintainer (56).

In another mechanism, the response-to-query receiver (74) stops receiving messages in response to queries. Since the messages are expected by the response-to-query receiver (74) in response to queries by the query sender (72), the response-to-query receiver (74) is aware when a message is expected but not received. When the response-to-query receiver (74) stops receiving the in-use messages, it causes de-allocation of the IP address from the user by updating memory (60) and the user identification maintainer (58) to indicate that the user is no longer active and by causing return of the IP address to the pool of IP addresses maintained by the IP address maintainer (56).

FIG. 3 is a process flow diagram showing the processes between and within a user, a network access server (NAS), and a home gateway server (HGS) in accordance with a specific embodiment of the present invention. At the beginning, in order to communicate over the Internet using the TCP/IP protocol, the user needs to obtain an IP address to identify himself on the Internet.

At 80, a connection is established between the user and the NAS. The connection may be made by using the common point-to-point protocol (PPP) or another suitable protocol. Once the connection is established, the user transmits and the NAS receives from the user authenticating information (82), usually in response to a challenge from the NAS. The authenticating information typically may include a user name and password, although other information may be used. The NAS may store the authenticating information in memory (84). Now, unless the NAS can authenticate the user locally, it needs to obtain authentication from another source. By using available information such as a table in local memory mapping specific users or specific user fully qualified domain names (FQDNs) to specific HGSes, the NAS determines the identity of the HGS that needs to be contacted for users to be authenticated in this manner (86). The NAS may also determine the HGS to be contacted by using the calling information (caller ID, for example) of the user.

Once the destination HGS has been identified, it is contacted by the NAS (88). The NAS may use the Remote Authentication Dial In Use Service (RADIUS) protocol or

another suitable protocol to contact the NAS. The NAS transmits, and the HGS receives from the NAS, the authentication information from the user (90).

After receiving the authenticating information, the HGS authenticates the user (92). This requires the HGS to check the authenticating information against information stored in memory. The HGS may proxy parts of the authenticating function to another server. In any case, the user is either authenticated or denied access based on the authentication process. Once authenticated, the HGS allocates an IP address from a pool maintained by the HGS to the user (94). The HGS then updates its memory (96). Such updating includes recording in a memory which IP address is allocated to the user, recording user identification information associated with the user, and recording that the IP address is not available for allocation to another user. This is important, as the HGS will use this stored information to de-allocate the IP address of the user when the HGS later determines that the user is no longer connected to its NAS.

The HGS then transmits the IP address back to the originating NAS (98). After receiving the IP address, the NAS updates its memory to associate the IP address with the user (100). Such updating may include updating routing tables where appropriate. The NAS then transmits the IP address to the user where it is received (102).

Once the user has obtained the IP address, the IP address is used to identify the user on the Internet. The user uses the IP address until its Internet connection is terminated, either by the user's intent or otherwise. Disconnection of the user from the

Internet may occur in several ways. Once disconnection occurs, the HGS must be made aware so that when the user's Internet connection stops the IP address can be de-allocated from the user and be made available to another user. The HGS must not be totally dependent on the NAS. For example, if the user's Internet connection stops because the NAS crashes, the HGS must still be able to de-allocate the IP address from the user.

FIG. 4 is a process flow diagram showing the processes between and within a user, a network access server, and a home gateway server if the connection between the NAS and the user is intentionally terminated by the user in accordance with a specific embodiment of the present invention. When the user wishes to intentionally terminate his Internet connection, the user may transmit a disconnection request which is received by the NAS (110). The NAS updates its memory to indicate that the IP address is no longer in use by the user (112). The NAS then generates and sends a disconnect notice to the HGS (114). Upon receiving the disconnect notice (116), the HGS also updates its memory to reflect that the user is no longer using the IP address (118).

It should be noted that steps 114 to 118 are not necessary if the NAS simply breaks off the connection between the user and the NAS in response to a disconnection request. In that case, the mechanisms described in FIGS. 5-7 below will result in implicit notification of the HGS of the user's disconnection.

FIG. 5 is a process flow diagram showing the processes between and within a user, a network access server, and a home gateway server when a NAS keep-alive sender

is used to monitor the status of an IP address in accordance with a specific embodiment of the present invention. Use of an NAS keep-alive sender is one way for the HGS to detect disconnection of the user from the Internet. This involves the NAS detecting an ongoing connection between itself and the user, and periodically sending keep-alive messages to the HGS indicating that the user is still connected. If the HGS stops receiving the periodic keep-alive messages, for any reason, the IP address is de-allocated from the user and returned to the pool.

At the beginning, the user is using the IP address (120). The NAS has a detector which detects an ongoing connection between the NAS and the user (122). The detector communicates with a keep-alive sender, which periodically sends keep-alive messages to the HGS for as long as the detector detects that user is connected to the NAS (124). The keep-alive messages are received by the HGS (126). As long as there is no failure in the system outside the HGS, the keep-alive messages will continue to be sent to the HGS (128) by repeating steps 122-126. However, if there is a system failure such as the NAS crashing or a break in the connection between the user and the NAS, the keep-alive messages will stop (130) and the HGS keep-alive receiver will stop receiving them (132). Since the HGS expects to receive the keep-alive messages periodically, the HGS will recognize discontinuation of the keep-alive messages and update its memory to reflect that the user is no longer using the IP address (134).

FIG. 6 is a process flow diagram showing the processes between and within a user, a network access server, and a home gateway server when a HGS query sender is

used to monitor the status of an IP address in accordance with a specific embodiment of the present invention. Use of an HGS query sender is a second way for the HGS to detect disconnection of the user from the Internet. This involves the HGS periodically sending a query as to whether the user is still using the IP address. The query may be answered by either the user or the NAS. Responding to the query by the NAS is illustrated.

At the beginning, the user is using the IP address (140). Periodically, the HGS query sender sends a query to the NAS as to whether the user is still using the IP address (142). If the NAS receives the query (143) and a detector at the NAS detects a connection between the NAS and the user (144), a responder at the NAS will send the HGS a positive confirmation of connection (146). If the confirmation is received by the HGS (148), the HGS will send another query after a period of time (142). If the HGS response-to-query receiver does not receive a positive confirmation of connection for any reason (150), the HGS will update its memory to reflect that the IP address is no longer being used by the user (152). By way of example, the HGS response-to-query receiver may not receive a positive confirmation of connection because the query was not received by the NAS (143), no connection was detected between the NAS and the user (144), or the positive confirmation was lost (148).

If the query is answered by the user, the functional components of the HGS remain the same. There will be a query sender that will periodically send queries and a response-to-query receiver that will cause memory to be updated if an expected response is not received.

FIG. 7 is a process flow diagram showing the processes between and within a user, a network access server, and a home gateway server when a user-originated in-use message is used to monitor the status of an IP address in accordance with a specific embodiment of the present invention. Use of a user-originated in-use message is a third way for the HGS to detect disconnection of the user from the Internet. This involves the user originating in-use messages which are periodically expected by the HGS.

At the beginning, the user is using an IP address (160). While there is a continuing connection, the user periodically sends in-use messages (162). An in-use message receiver at the NAS receives the messages (163). A forwarder at the NAS forwards the messages to the HGS (164). For as long as the HGS in-use receiver receives the periodic in-use messages (166), steps 162 to 164 are repeated. If, for any reason, the HGS in-use receiver stops receiving the periodic in-use messages, the HGS will update its memory to indicate that the user is no longer using the IP address (168).

While the invention has been described for use by a single user, it will be apparent to those skilled in the art having the benefit of this disclosure that both the NAS and the HGS can simultaneously serve multiple users by employing the invention.

It will also be apparent that the functional components of the NAS and the HGS may be implemented in a variety of ways. For example, they may be implemented in the form of program storage devices readable by a machine and tangibly embodying a

program of instructions executable by the machine to perform the methods described herein. Such implementations may include a variety of operating systems, computing platforms, and/or computer languages. In addition, those of ordinary skill in the art will readily recognize that devices such as hardwired devices, devices relying on FPGA (field programmable gate array) or ASIC (application specific integrated circuit) technology, or the like, may also be used without departing from the scope and spirit of the inventive concepts described herein.

While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art having the benefit of this disclosure that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention, therefore, is not to be restricted except in the spirit of the appended claims.